



FORUM SENTRY™ VERSION 9

WEB-BASED ADMINISTRATION GUIDE

Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Sentry™ Web Services Security Gateway, Presidio™ OpenPGP Security Gateway, Forum FIA Gateway™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 Web-based Administration Guide, published July 2024.

D-ASF-SE-873094

Table of Contents

INTRODUCTION TO THE WEB-BASED ADMINISTRATION GUIDE	1
LOG IN AND LOGOUT	3
METHODS TO CONTROL ACCESS TO WEBADMIN.....	5
CHANGE DEFAULT WEBADMIN SSL/TLS CERTIFICATE	5
SUPERUSER OR PRIVILEGED ACCESS.....	13
ADMINISTRATION DOMAIN.....	13
NAVIGATION	15
COMMON OPERATIONS IN THE WEBADMIN	20
APPENDIX	22
INDEX	25

INTRODUCTION TO THE WEB-BASED ADMINISTRATION GUIDE

Audience for the Web-based Administration Guide

The *Forum Systems Sentry™ Version 9 Web-based Administration Guide* is a guide for System Administrators. This document includes:

An overview of the WebAdmin User Interface.

- How to login and log out.
- A description of the Getting Started page.
- How to create a secure session.
- Use your corporate TLS Key Pair to create a secure session.
- How to navigate the WebAdmin.
- How to access help files.
- How to perform common operations in the WebAdmin.

Conventions Used in the Web-based Administration Guide

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum API Security Gateway™ is referred to as the Sentry, 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

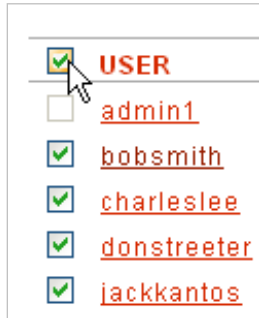
- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

Universal Select All and De-select All Convention



On a number of screens, you may select all of the elements listed by clicking the topmost checkbox once that prefaces the category name.

You may de-select all of the elements listed by again clicking the topmost checkbox that prefaces the category name.

Overview

The WebAdmin is a web-based management interface used for monitoring as well as configuring all aspects of the system including server, security and network policies. Access to the WebAdmin UI is available after your IT Administrator has completed installation.

TLS Security

The WebAdmin UI comes TLS-enabled via a pre-loaded Certificate that requires no configuration. The WebAdmin UI communicates via the HTTPS transport protocol.

LOG IN AND LOGOUT

Log in

Log in to Forum Sentry from your browser with an HTTP request to the IP:port configured during installation. By default, the port used is 5050.

<https://<IP>:5050>

A web form titled "FORUM SYSTEMS LOGIN". It has two input fields: "User Name*" with the text "admin1" and "Password*" with masked characters "*****". To the right of the password field is a red "Login" button. A mouse cursor is pointing at the "Login" button.

- With your browser open, enter the **URL** supplied by your IT Administrator to access the Forum Systems WebAdmin UI. A Security Alert message appears with the default SSL certificate.
- Press **Yes** to accept the certificate. The Login screen appears.
- The Enter Network Password screen appears.
- Enter a WebAdmin **User Name** and **Password**, and then click **Login**. The WebAdmin appears, displaying the Getting Started screen.

Logout

Logout of the WebAdmin while on any screen by clicking the LOGOUT button on the lower right of the screen.



Access Online Help

From the WebAdmin, select the Help link to view the HELP screen. Select the Online Help link to open up Help.



Access Context-sensitive Help

At the top right of the screen, select the ? to view the context-sensitive Help for the opened WebAdmin screen.



Session Timeout Duration

The default session timeout is set to 8 minutes. To increase this value, under the Settings category of the Navigator, navigate to the SYSTEM screen and increase the Session Timeout (in minutes) up to **120** minutes by entering this value in the Session Timeout field, and clicking **Save**.

Execute Commands with Hot Keys

While executing a command, you may use any Hot Key designated on a command menu instead of clicking a command button. The following example displays how to delete using Hot Keys.



METHODS TO CONTROL ACCESS TO WEBADMIN

Forum Sentry is designed with several aspects of controlling the ability to administer the policies via the WebAdmin. These include:

1. Physical dedicated network interface. This allows restricting access for management traffic to the WebAdmin only on dedicated networks able to communicate with the separate management interface.
2. IP Access Control. This enables restricting access to the management IP and Port based on the designated set of Allowed or Denied IP source addresses. Connection attempts to the WebAdmin IP and Port are first checked based on the source IP as to whether to allow the connection.
3. TLS Certificate with One-Way or 2-Way SSL. Enables the use of a designed SSL policy with corporate key pair that further can be configured to require 2-way SSL client X.509 authentication to ensure administrators authenticate using an X.509 in order to establish an SSL session.
4. Password Control. Enables designating which Administrative users are allowed to access the machine
5. Role Based Administration. This mechanism filters available policy items based on the administrator credentials provided allowing different administrators of Sentry to have different views and rights as to which policies can be visible, created, modified, and deleted.
6. Multi-Factor Authentication. This can be configured via Okta or other MFA providers.

CHANGE DEFAULT WEBADMIN SSL/TLS CERTIFICATE

Your corporate security policies may dictate that your system settings be configured using your own corporate Key Pair to secure the SSL connection between your corporate web browser and the system. This is accomplished by:

1. Physically installing the system.
2. Logging on to the WebAdmin UI.
3. Importing your corporate PKCS#1 or PKCS#12 key pair into the Keys screen.
4. Creating an SSL Termination policy with the corporate key pair.
5. Reconfiguring the system by selecting your specific corporate SSL Termination policy to apply to the system.

Steps 3 (Import a PKCS#1 or #12 Key Pair), 4 (Create an SSL Termination Policy) and 5 (Configure System Settings with your Own SSL Termination Policy) are detailed next:

Note: For more information on physically installing the system, refer to the *Forum Systems Sentry™ Version 9 Hardware Installation Guide*.

For more information on initially logging on to Forum Sentry, refer to the Logon section of this document. For more information on PKCS keys and SSL Termination Policies, refer to the PKCS Keys and SSL Policies section of the *Forum Systems Sentry™ Version 9 Security Policies and PKI Guide*.

For more information on Forum Sentry system settings, refer to the System Settings section of the *Forum Systems Sentry™ Version 9 System Management Guide*.

Import a PKCS 12 Key Pair

Importing a PKCS#1 or PKCS#12 key pair requires that you have both the public key certificate and the private key in your file system. This example displays importing a PKCS#12 key pair.

KEYS

Show Full View

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS
<input type="checkbox"/>	PGP_Dave	OpenPGP Key Pair	1024/2048	Active
<input type="checkbox"/>	PGP_DaveM	OpenPGP Key Pair	1024/3072	Active
<input type="checkbox"/>	PGP_Jeff	OpenPGP Public Key	1024/1536	Active
<input type="checkbox"/>	PGP_Sandy	OpenPGP Key Pair	1024/1536	Active

4 items found. Search , max results

Show

Settings

Delete

Import

New

6

I Forum Sentry™ Web-based Administration Guide

KEYS > KEY IMPORT

PKCS#12 KEY PAIRS

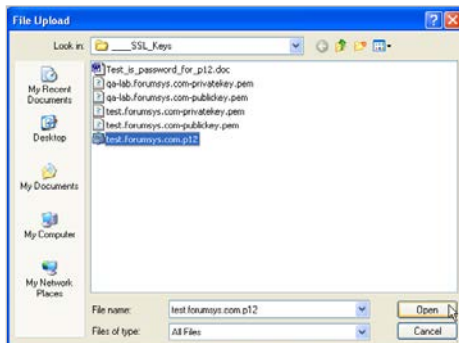
Name*:

Private Key and Public Certificate*:

Private Key Passphrase:

File Integrity Password:

Create Signer Group from Certificate Chain: ☒



KEYS > KEY IMPORT

PKCS#12 KEY PAIRS

Name*:

Private Key and Public Certificate*:

Private Key Passphrase:

File Integrity Password:

Create Signer Group from Certificate Chain: ☒

KEYS

[Show Full View](#)

<input type="checkbox"/>	NAME	TYPE	SIZE	STATUS
<input type="checkbox"/>	ABC_Corp_SSL	Key Pair	1024	Active
<input type="checkbox"/>	ABC_Corp_SSL_cert	Certificate	1024	Active
<input type="checkbox"/>	Danielle	Key Pair	2048	Active
<input type="checkbox"/>	Danielle_cert	Certificate	2048	Active
<input type="checkbox"/>	NewHampshire	Key Pair	512	Active
<input type="checkbox"/>	NewHampshire_0_cert	Certificate	512	Active
<input type="checkbox"/>	NewHampshire_1_cert	Certificate	2048	Active
<input type="checkbox"/>	PGP_Dave	OpenPGP Key Pair	1024/2048	Active
<input type="checkbox"/>	PGP_DaveM	OpenPGP Key Pair	1024/3072	Active
<input type="checkbox"/>	PGP_Jeff	OpenPGP Public Key	1024/1536	Active

14 items found. Search , max results

- Navigate to the **Keys** screen.
- Click **Import**.
- Click the **PKCS#12 Key Pairs** radio button, and then click **Next**.
- In the Name field, enter a **name** for this key.
- Click **Browse** aligned with the Private Key and Public Certificate field. The Choose file screen appears. Navigate your file system and click a **PKCS#12 Key Pair**, then click **Open**. The key pair populates the File name field, and the screen closes.
- The PKCS#12 KEY PAIRS screen re-appears. If, when initially creating your Key Pair, you had also created a password, enter this password in the **Private Key Passphrase** field.
- If, when initially creating your Key Pair, you had also created a File Integrity Password, enter this password in the **File Integrity Password** field.
- Confirm that the **Create Signer Group from Certificate Chain** checkbox is checked.
- Click **Submit**.

Navigate to the **Signers Group** screen to view the new signer group.

SIGNER GROUPS

<input type="checkbox"/>	SIGNER GROUP
<input type="checkbox"/>	<u>DEFAULT</u>
<input type="checkbox"/>	<u>ABC Corp SSL</u>
<input type="checkbox"/>	<u>Danielle Group</u>
<input type="checkbox"/>	<u>Jack Group</u>
<input type="checkbox"/>	<u>Mark Group</u>
<input type="checkbox"/>	<u>NewHampshire</u>

6 items found. Search , max results

Create an SSL Termination Policy

SSL POLICIES

☐ **SSL INITIATION POLICY**

☐ [SSL Init](#)

☐ [SSL Init NH](#)

☐ [SSL Init Walter](#)

☐ [SSL Policy_527873370](#)

☐ **SSL TERMINATION POLICY**

☐ [SSL Policy_Joyce](#)

☐ [SSL Term_Danielle](#)

☐ [SSL Term_NH](#)

3 items found. Search , max results [Show](#) [Delete](#) [New](#)

SSL POLICIES > NEW SSL POLICY

SSL POLICY TYPE

☐ Initiation

☒ Termination

[Next](#)

SSL POLICIES > SSL TERMINATION POLICY

SSL POLICY

Name:

SSL TERMINATION

Key Pair: [Edit](#)

Authenticate the Client: ☒

Signer Group: [Edit](#)

Associate subject DN to a user: ☐

 Use user attribute only (cn or uid): ☐

 ACL Policy:

Use cipher suites order: ☐

☐ PROTOCOL

- ☒ TLSv1.2
- ☒ TLSv1.1
- ☐ TLSv1
- ☐ SSLv3
- ☐ SSLv2Hello

[Save](#)

[Hide cipher suites](#)

CIPHER SUITE FILTERS

- ☒ RSA ☒ DSS ☒ ECDSA
- ☒ DHE ☒ ECDH ☒ ECDHE
- ☒ AES ☒ 3DES ☒ RC4 ☒ 128 ☒ 256 ☐ Vulnerable

Drag & drop the enabled cipher suites to reorder their priority

<input type="checkbox"/>	CIPHER SUITE	OPENSSL NAME
<input checked="" type="checkbox"/>	1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
<input checked="" type="checkbox"/>	2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA

SSL POLICIES

☐ **SSL INITIATION POLICY**

☐ [SSL_Init](#)

☐ [SSL_Init_NH](#)

☐ [SSL_Init_Walter](#)

☐ [SSL_Policy_527873370](#)

☐ **SSL TERMINATION POLICY**

☐ [SSL_Policy_Joyce](#)

☐ [SSL_Term_ABC_Corp](#)

☐ [SSL_Term_Danielle](#)

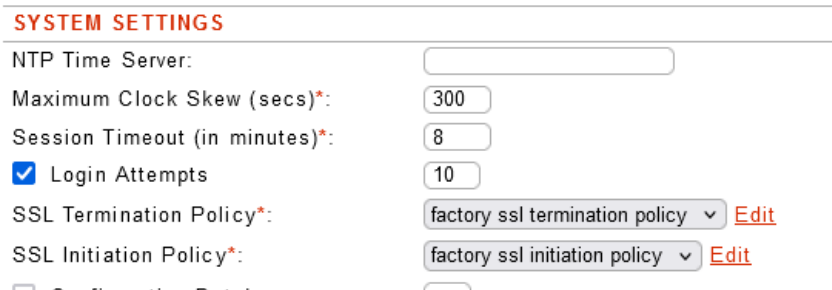
☐ [SSL_Term_NH](#)

4 items found. Search , max results 1000 [Show](#) [Delete](#) [New](#)

- Navigate to the **SSL Policies** screen.
- Click **New**.
- Select the **Termination** radio button, and then click **Next**. The SSL TERMINATION POLICY screen appears with a pre-populated policy name in the Policy Name field.
- Overwrite this name and enter a **unique SSL Policy Name** in the SSL Policy Name field.
- From the SSL TERMINATION section of the screen, in the Key Pair drop down list, select a system **Key Pair Alias** to bind to this SSL Policy.
- Check the **Authenticate the Client** checkbox.
- Select a Signer Group from the Signer Group drop down list.
- Skip the Associate subject DN to a user checkbox.
- Skip the ACL Policy drop down list option.
- From the PROTOCOL section, check one or more of the TLS or SSL options shown. Note: it is recommended that only TLS 1.2 is used.
- From the CIPHER SUITE section, check all the **checkboxes** prefacing the cipher suites that should be applied during the SSL/TLS authentication. These will be filled in by default based on the protocol settings and recommended ciphers.
- Click **Create**.

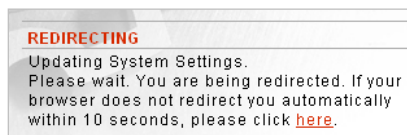
Reconfigure System Settings with Your Corporate SSL/TLS Certificate

Reconfigure the System screen by selecting your own specific SSL Termination policy and save the system configuration. It is best to allow only users who are very familiar with your system change these settings, if required. Follow these steps to reconfigure the system:



The screenshot shows the 'SYSTEM SETTINGS' section of a web administration interface. It contains several configuration fields: 'NTP Time Server' with an empty text box; 'Maximum Clock Skew (secs)*:' with a value of 300; 'Session Timeout (in minutes)*:' with a value of 8; a checked checkbox for 'Login Attempts' with a value of 10; 'SSL Termination Policy*:' with a dropdown menu set to 'factory ssl termination policy' and an 'Edit' link; and 'SSL Initiation Policy*:' with a dropdown menu set to 'factory ssl initiation policy' and an 'Edit' link. At the bottom, there are navigation icons for back, home, and other functions.

- From the WebAdmin, select the **System** screen.
- From the SSL Termination Policy drop down list, select your corporate **SSL Termination policy**.
- Click **Save**. The REDIRECTING screen appears, and the SYSTEM SETTINGS screen refreshes.



SUPERUSER OR PRIVILEGED ACCESS

The default Administrator created on the system has privileged access rights. An Administrator with privileged access rights is referred to as a superuser. A superuser is afforded the privilege of creating any type of policy on the system. A User is granted superuser privileges by first clicking on one of the users and then checking the **Enable privileged access** setting on the USER DETAILS screen as shown in the graphic below.

USER MANAGEMENT > USER DETAILS

USER DETAILS

User Name: charleslee

Password:

Confirm Password:

ADVANCED PROPERTIES

☒ Store recoverable passwords as well as password hashes (required in certain feature configurations)

☒ Enable privileged access

☐ Restrict Menus

Role policy:

Email:

Signer Key: [None]

DN Alias:

SSH Public Key: [None]

USER GROUPS

- ☐ Group1
- ☐ Group2
- ☐ Group3
- ☐ SNMPPMonitor

A Superuser can create policies under any of the defined Roles. When a Superuser creates policies, these policies are created under the current Active Domain as shown on the bottom right of the screen. A Superuser has access to all of the policies for all of the Domains on the system.

Caveats with Superusers

When working as a Superuser in the system, consider:

- One Superuser cannot restrict another superuser.
- Any Superuser user can restrict a non-superuser.

Note: For more information on users, refer to the Users section of the *Forum Systems Sentry™ Version 9 Access Control Guide*.

ADMINISTRATION DOMAIN

The Active Domain is displayed at the bottom of the WebAdmin UI. After installation of the system, the default Domain, labeled Default, is visible.

Active Domain:

Note: For more information on the Active Domain, refer to the Overview of MultiDomain Administration and the Domains sections of the *Forum Systems Sentry™ Version 9 Access Control Guide*.

NAVIGATION

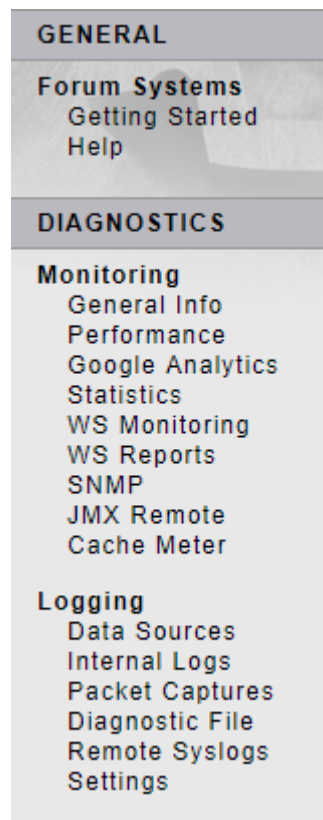
The Navigator, on the left side of the WebAdmin UI, includes collapsible categories. Note that categories and items may be based on the configured administrator role, the specific release version, and the licensed feature set.



The main categories of the Navigator may be expanded or compressed. Based on your licensed feature set and your privileges access, the WebAdmin UI may have some or all of these screens, the contents of which are described next:

The Navigator

Each category in the Navigator is grouped with associated functions.



The GENERAL category includes the following:

- The Getting Started screen provides a quick link to four screens and access to the Import and Validate WSDL Documents wizard.
- The Help screen displays online help.

The DIAGNOSTICS category includes the following:

- The General Info screen displays system/application memory and enabled Network policies.
- The Performance screen displays more detailed system performance statistics than provided on the General Info screen.
- The Statistics screen displays system document processing metrics.
- The Web Services (WS) Monitoring screen displays all WSDL and XML policy activities.
- The Web Services (WS) Reports screen manages the creation, scheduling and email delivery of reports in data or chart form for WSDL and XML Policies.
- The SNMP screen manages SNMP security configuration settings and contains links to MIB files for easy retrieval.
- The JMX Remote screen manages statistics and configuration settings.
- The Cache Meter screen displays caching statistics in chart form and provides a table of cached objects.
- The Data Sources screen manages archiving policies for Oracle,

MySQL or DB2 databases.

- The Internal Logs screen provides views of System & Audit logs.
- The Packet Capture screen manages capturing and downloading full TCP packets for network diagnosis.
- The Diagnostic File screen manages captured system diagnostics files.
- The Remote Syslogs screen manages Syslog Logging policies for up to six remote syslog destinations.
- The Settings screen manages individual settings for each log.

GATEWAY

Network Policies

Network Policies
Proxy Policies
Cloud Policies

WSDL Policies

WSDL Libraries
WSDL Policies

Content Policies

XML Policies
REST Policies
JSON Policies
HTML Policies
STS Policies
OAuth Policies
Tests

Task Policies

Task List Groups
Task Lists

Redirect Policies

Redirect Policies

Request Filters

Request Filters

The GATEWAY category includes the following:

- The Network Policies screen manages HTTP(S) Listener and Remote policies, Group Remote, FTP Network and FTP User policies (that allow for bulk encryption and bulk decryption with OpenPGP over FTP), SMTP Tibco-Rendezvous, Tibco-EMS and IBM MQ policies.
- The Proxy Policies screen manages the proxy policies which can be used when an Internet connection requires a proxy server.
- The WSDL Libraries screen manages WSDL aggregation.
- The WSDL Policies screen manages WSDL policies.
- The XML Policies screen manages XML policies.
- The REST Policies screen manages REST policies.
- The JSON Policies screen manages JSON policies.
- The HTML Policies screen manages HTML policies.
- The STS Policies screen manages STS policies. This screen is not always available with all Sentry licenses.
- The OAuth Policies screen manages OAuth policies.
- The Tests screen manages test policies.
- The Tasks List Groups screen manages collections of Task Lists as reusable Task List Groups.
- The Tasks Lists screen manages global Task Lists that may be re-applied to WSDL and XML policies.
- The Redirect Policies screen manages the Redirect Policies.
- The Request Filters screen manages the Request Filter policies.

RESOURCES

PKI

- Keys
- Signer Groups
- CRLs
- SSH Keys
- Known Hosts

Security Policies

- OpenPGP
- SSL
- Encryption
- Decryption
- Signature
- Verification

Pattern Match

- Pattern Match

Templates

- Error Templates

Documents

- Documents

WAF

- WAF Policies
- Value Types

The RESOURCES category includes the following:

- The Keys screen manages Key Pairs and Public Certificates for PKCS and OpenPGP keys, import and key generation.
- The Signer Groups screen manages Signer Group policies for X.509 path validation.
- The CRLs screen handles Certificate Revocation List policies.
- The SSH Keys manages the SSH Keys.
- The Known Hosts screen manages the known hosts.
- The OpenPGP Policies screen manages OpenPGP Encryption, Decryption, Signing and Verification policies.
- The SSL Policies screen manages SSL Termination and SSL Initiation policies.
- The Encryption screen manages Encryption policies.
- The Decryption screen manages Decryption policies.
- The Signature screen manages Signature policies.
- The Verification screen manages Verification policies.
- The Pattern Match Policies screen manages policies that search and replace defined patterns in XML documents of a WSDL policy.
- The Templates screen manages the creation of custom error handling on Network policies.
- The Documents screen provides a collection of all sample XML documents.
- The WSRM Policies screen manages the WSRM Policies.
- The WAF Policies screen manages the WAF policies.
- The Value Types screen manages the Value Type policies.

IDP

IDP Blocking

- IDP Blocking

IDP Policies

- IDP Rules
- IDP Groups
- IDP Actions
- IDP Schedules
- IDP Clustering

The IDP category includes the following:

- The IDP Blocking screen is a listing of all currently blocked or throttled users or IPs.
- The IDP Rules screen manages individual IDP Rules.
- The IDP Groups screen manages groups of IDP Rules.
- The IDP Actions screen manages actions which IDP rules may trigger.
- The IDP Schedule screen manages a programmed schedule for IDP Rules.
- The IDP Clustering screen manages the persistent IDP configuration.

ACCESS

Runtime Access

User ACLs
IP ACLs

Admin Access

Domains
Roles

User Policies

Users
Cache
User Groups
Active Users
LDAP
RSA SecurID
Kerberos
SiteMinder
TAM
WebSeal
Oracle AM
WS-Trust
OpenAM
REST
Sentry
Custom

The ACCESS category includes the following:

- The User ACLs screen manages Access Control Lists of resources or organizations and membership privileges for Groups of Users.
- The IP ACLs screen manages global Access Control List policies that define IP ranges for HTTP/S and SMTP listener policies in the system as well as WebAdmin IP access control.
- The Domains screen manages access control for design-time.
- The Roles screen manages which screens that users may access based on their Role in the system.
- The Users screen manages User policies and privileges.
- The Cache screen manages the cache settings.
- The User Groups screen manages groups and sub-groups and their membership privileges. This screen also manages System groups.
- The Active Users screen manages all users on the product.
- The LDAP screen manages dynamic LDAP users, represented as groups for use within the system.
- The Kerberos screen manages access control with WSDL and XML policies which use Kerberos tickets.
- The SiteMinder screen manages SiteMinder users and groups for system policy identity management.
- The TAM screen manages IBM Tivoli Access Manager users and groups for system policy identity management.
- The Oracle AM screen manages Oracle Access Manager™ users and groups for system policy identity management.
- The ClearTrust screen manages access control with RSA ClearTrust® users and groups for system policy identity management.
- The HP SelectAccess screen manages HP SelectAccess users and groups for system policy identity management.
- The WS-Trust screen manages WS-Trust users and groups for system policy identity management.
- The OpenAM screen manages the Sun JSAM policies.
- The REST screen manages REST Identity policies.

SYSTEM
Settings System Control Preferences Network
Configuration Export Import Compare Backup Agents Agent Groups Upgrade REST API Overview

The SYSTEM category includes the following:

- The System screen manages system-wide settings.
- The Control screen manages Shutdown and Reboot commands.
- The Preferences screen provides a global configuration setting for allowing Process Response to be enabled by default.
- The Network screen manages your network configuration settings
- Export screen manages exporting and transferring system configuration files among systems.
- The Import screen manages importing of system configuration files. . Also supported are GDM Imports (importing WSDL, XML, REST, JSON, HTML, STS, and OAuth policies and their dependencies) into the system.
- The Backup screen manages system backup settings.
- The Agents screen manages profiles between the Policy Server (MASTER) machine and any Agent machines.
- The Agent Groups screen manages a collection of individual Agent profiles assembled into GDM Agent groups.
- The Upgrade screen manages software upgrades.
- The REST API screen manages the REST API configuration on the system.
- The Overview screen provides a menu system for more granular selection of policies for GDM export.

PARTNERS
Partners Clam AV ICAP AV

The PARTNERS category includes the following:

- The Clam AV screen is for configuring CLAM's antivirus on the system.
- The ICAP AV screen is for configuring antivirus or other malware scanning capability over the ICAP protocol

Note: Based on which licensed features your system includes, some screen elements in the Navigator will not appear.

COMMON OPERATIONS IN THE WEBADMIN

A variety of operations that are common across the system are also performed in a similar manner. These are:

- Create an Initial Policy.
- Edit or View a Policy.
- Enable or Disable a Policy.
- Filter Display with Search Field.
- Filter Display with Max Results Field.
- Delete a Policy.

Rather than repeat these common operations that are performed in the same manner throughout the WebAdmin, they are summarized next:

Create an Initial Policy

On some screens, only after you create your first policy will you see the table and table headers under which this policy will be listed.

Before Creating First HTTP or HTTPS Policy

NETWORK POLICIES						
No items to display						
<div>DeleteEnableDisableNew</div>						

After Creating First HTTP or HTTPS Policy

NETWORK POLICIES						
HTTP Listener Policies						
<input type="checkbox"/>	NAME	STATUS	PROTOCOL	LISTENER ADDRESS	AUTHENTICATION	ACL
<input type="checkbox"/>	+ HttpListenerPolicy-0	●	HTTPS	10.5.6.92:443	SSL Client Auth	Default
<div>DeleteEnableDisableNew</div>						

Edit or View a Policy

- Navigate to the **desired** screen.
- Click a **Policy name** link and a DETAILS screen appears.
- Perform desired edits.
- Click **Save**.

Enable or Disable a Policy

- Navigate to the **desired** screen.
- Check the **checkbox** aligned with a **name** link to toggle enabling/disabling. The status light turns green for enabled policies and red for disabled policies.

Filter Display of Policies with Search Field

- Navigate to the **desired** screen.
- In the search field, enter one (or more) alphabetic or numeric **characters** to view the records matching the alphabetic or numeric characters.
- Click **Show**.

Filter Display of Policies with Max Results Field

- Navigate to the **desired** screen.
- In the max results field, enter a **number** for the number of records to display.
- Click **Show**.

Delete a Policy

- Navigate to the **desired** screen.
- Check the **checkbox** to the left of a **name** link.
- Click **Delete** and a system message appears. Reply by clicking **OK**.

Note: Some policies can only be deleted after they have been disassociated from other policies

Remove a Policy

- Navigate to the **desired** screen.
- Check the **checkbox** to the left of a **name** link.
- Click **Remove** and a system message appears. Reply by clicking **OK**.

APPENDIX

Appendix A - Specifications in Web-based Administration Guide

ELEMENT SUPPORTED	SPECIFICATIONS
System Session Timeout	Default is 8 minutes; however minimum allowed is 1 minute and maximum allowed is 120 minutes.
Network Configuration	Only a single network configuration is allowed on each System at one time.
Transport Protocols	<ul style="list-style-type: none">• Amazon S3• AMQP 1.0• FTP / FTPS (FTP over SSL and FTP over TLS)• HTTP / HTTPS• RabbitMQ• SFTP• SMTP• ActiveMQ• Tibco-EMS• JBoss• IBM MQ• Sun Java MQ• WebLogic• Solace JMS
Import / Export Configuration files	Only a single System configuration (filename.fsx) file is active at any given time.
Log Config	The default Log Lifespan (in days) is 15.
Log File Size	The default log file size is 1024 MB
Remote Syslog	Up to six servers can be specified to be forwarded syslog datagrams.
Enabled WSDL and XML Policies at one time	Unlimited *
Enabled WSDL Libraries at one time	Unlimited *
Agent machines supported	Unlimited *
Agent groups supported	Unlimited *
Enabled Listener or Remote Network Policies at one time	Unlimited *
Max number of configured data or charted reports in the system at one time	Unlimited *

Max number of scheduled data or charted reports in the system at one time	Unlimited *
---	-------------

ELEMENT SUPPORTED	SPECIFICATIONS
HTTP/S Listener Policies and HTTP/S Remote Policies	Network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
Group Remote Network Policies	Network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
SMTP Network policies	SMTP network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
FTP Network Policies and FTP over SSL/TLS Network Policies	Network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
Concurrent connections per FTP Network Policy	8-1024
FTP User Policies and FTP over SSL/TLS User Policies	The number of FTP User Policies on one FTP Network Policy is unlimited.
Tibco Rendezvous and Tibco EMS Remote Policies with and without SSL.	Network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
MQ Listener and MQ Remote Policies with and without SSL.	Network policies share system resources; therefore, Forum Systems recommends limiting the number of active Network policies to 32.
Global Tasks Lists	Unlimited *
Global Task List Groups	Unlimited *
Documents	Unlimited *
Templates for Error Handling	Unlimited *
Database Connections	99
Database Support	Oracle 9i, 10g, Oracle RAC 10g, MySQL V3.23.36 or higher, DB2 7.2 (DB2 9**).

ELEMENT SUPPORTED	SPECIFICATIONS
PKCS Key Size	10124 – 4096 bits.
OpenPGP Key Size	1024-4096 bits
Maximum number of PKCS Keys supported by the system	1000
Maximum number of OpenPGP Keys supported by the system	1000
CRL Policies	Unlimited *
SSL Policies	Unlimited *
OpenPGP Encryption, OpenPGP Decryption, OpenPGP Signing and OpenPGP Verification Policies	Unlimited *
XML Encryption, XML Decryption, XML Signing and XML Verification Policies	Unlimited *
Pattern Match Policies	Unlimited *
SiteMinder Policies	Unlimited *
Tivoli Policies	Unlimited *
User Policies	Unlimited *
Groups Policies	Unlimited *
User ACL Policies	Unlimited *
IP ACL Policies	Unlimited *
Role Policies	Unlimited *
Domain Policies	Unlimited *

* Limited only by disk space.

** Available with patch upgrade.

INDEX

configure system settings using your own corporate key pair	5	import a PKCS#1 key pair	5
context-sensitive Help	4	import a PKCS#12 key pair	5
conventions used	1	log in	3
De-select all convention	2	logout	3
HTTPS		Navigator	15
supported on WebAdmin UI	2	online Help	3
		PKCS#1 key pair	

importing	5
PKCS#12 key pair	
importing	5
recommended system settings	
increase session timeout	4
secure session :configure system settings using	
your own corporate key pair	5
Select all convention	2
Session Timeout	
increase session timeout	4
SSL-enabled	

WebAdmin UI	2
superuser	13
superuser privilege.....	13
transport protocols supported in WebAdmin UI.	2
universal De-select all convention	2
universal Select all convention	2
Web Admin	
panes.....	15
WebAdmin UI	
SSL-enabled.....	2